



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/737,742	12/18/2000	Tonnes Brekne	198443US2	1337

22850 7590 01/06/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.  
1940 DUKE STREET  
ALEXANDRIA, VA 22314

EXAMINER

LANIER, BENJAMIN E

ART UNIT PAPER NUMBER

2132

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/737,742

Applicant(s)

BREKNE, TONNES

Examiner

Benjamin E Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-67 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_ is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☒ Claim(s) 1-67 are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

## **DETAILED ACTION**

### ***Election/Restrictions***

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
  - I. Claims 1-8, drawn to a method for creating an augmented Mealy machine, classified in class 716, subclass 18.
  - II. Claims 9-12, drawn to a method of converting a Blum-Shub-Smale machine, classified in class 716, subclass 3.
  - III. Claims 13-17, drawn to a method of transforming a BBS machine to a multivariate polynomial mapping, classified in class 713, subclass 3.
  - IV. Claims 18-23, 33, 54 drawn to a method of specifying a pattern of encryption of multivariate mappings, classified in class 380, subclass 28.
  - V. Claims 26-29, 40-42, 59, drawn to a method of generating re-encryption keys, classified in class 380, subclass 44.
  - VI. Claims 24-25, 39, drawn to a method of encrypting plural variables and mapping components of multivariate mappings, classified in class 380, subclass 28.
  - VII. Claims 30, 31, drawn to a method of converting a mapping into a function, classified in class 708, subclass 492.
  - VIII. Claim 45, drawn to a Turing platform, classified in class 712, subclass 201.
  - IX. Claims 47-51, drawn to a register machine, classified in class 712, subclass 2.
  - X. Claims 55-58, 61-67, drawn to a method of generating keys for parametrized multivariate encryption of multivariate mappings, classified in class 380, subclass 44.

- XI. Claim 60, drawn to a method of specifying an encryption pattern for parametrized encryption of a register machine, classified in class 380, subclass 28.
- XII. Claims 34-38, drawn to a method of generating keys for multivariate encryption of multivariate mappings, classified in class 380, subclass 44.
- XIII. Claims 32, 43, 44, 52, 53, drawn to a method of symbolically composing mappings, classified in class 708, subclass 400.
- XIV. Claim 46, drawn to a method of computing with a host running a Turing platform, classified in class 712, subclass 203.

2. The inventions are distinct, each from the other because of the following reasons:

Inventions I-XIV are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such as a synthesizer for logic circuits. In the instant case, invention II has separate utility such as a logic circuit converter. In the instant case, invention III has separate utility of creating mappings from logic circuits. In the instant case, invention IV has separate utility such as an encryptor. In the instant case, invention V has separate utility such as a cryptographic key generator. In the instant case, invention VI has separate utility such as an encryptor. In the instant case, invention VII has separate utility such as a mapping converter. In the instant case, invention VIII has separate utility such as a data flow based system. In the instant case, invention IX has separate utility such as a vector processor. In the instant case, invention X has separate utility such as a key generator. In the instant case, invention XI has separate utility such as a method for encryption. In the

Art Unit: 2132

instant case, invention XII has separate utility of key generation for multivariate encryption of multivariate mappings. In the instant case, invention XIII has separate utility of symbolically composing mappings. In the instant case, invention XIV has separate utility of computing on a host running a Turing platform. See MPEP § 806.05(d).

3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

4. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Groups II-XIV, restriction for examination purposes as indicated is proper.

5. Because these inventions are distinct for the reasons given above and the search required for Group II is not required for Group I, III-XIV, restriction for examination purposes as indicated is proper.

6. Because these inventions are distinct for the reasons given above and the search required for Group III is not required for Group I, II, IV-XIV, restriction for examination purposes as indicated is proper.

7. Because these inventions are distinct for the reasons given above and the search required for Group IV is not required for Group I-III, V-XIV, restriction for examination purposes as indicated is proper.

Art Unit: 2132

8. Because these inventions are distinct for the reasons given above and the search required for Group V is not required for Group I-IV, VI-XIV, restriction for examination purposes as indicated is proper.

9. Because these inventions are distinct for the reasons given above and the search required for Group VI is not required for Group I-V, VII-XIV, restriction for examination purposes as indicated is proper.

10. Because these inventions are distinct for the reasons given above and the search required for Group VII is not required for Group I-VI, VIII-XIV, restriction for examination purposes as indicated is proper.

11. Because these inventions are distinct for the reasons given above and the search required for Group VIII is not required for Group I-VII, IX-XIV, restriction for examination purposes as indicated is proper.

12. Because these inventions are distinct for the reasons given above and the search required for Group IX is not required for Group I-VIII, X-XIV, restriction for examination purposes as indicated is proper.

13. Because these inventions are distinct for the reasons given above and the search required for Group X is not required for Group I-IX, XI-XIV, restriction for examination purposes as indicated is proper.

14. Because these inventions are distinct for the reasons given above and the search required for Group XI is not required for Group I-X, XII-XIV, restriction for examination purposes as indicated is proper.

Art Unit: 2132

15. Because these inventions are distinct for the reasons given above and the search required for Group XII is not required for Group I-XI, XIII, XIV, restriction for examination purposes as indicated is proper.

16. Because these inventions are distinct for the reasons given above and the search required for Group XIII is not required for Group I-XII, XIV, restriction for examination purposes as indicated is proper.

17. Because these inventions are distinct for the reasons given above and the search required for Group XIV is not required for Group I-XIII, restriction for examination purposes as indicated is proper.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 703-305-7684. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

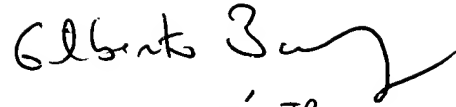
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703)305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit: 2132



Benjamin E. Lanier



GILBERTO BARRÓN JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100